PATENT ABSTRACTS OF JAPAN

(11)Publication number : 62-254543
(43)Date of publication of application : 06.11.1987

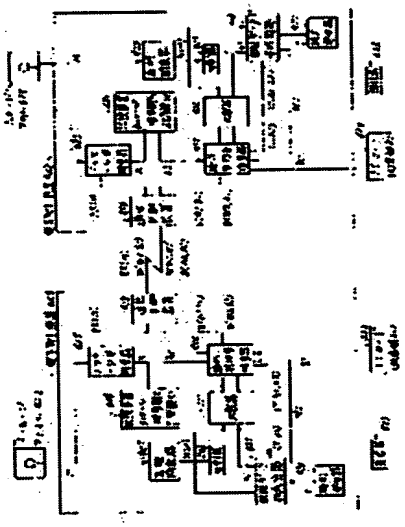
(51)Int.Cl. H04L 9/00
// G06F 15/30

(21)Application number : 61-096705
(22)Date of filing : 28.04.1986

(71)Applicant : HITACHI LTD
(72)Inventor : TAKARAGI KAZUO
KURASHIKI NOBUHIRO
SASAKI RYOICHI
SHIRAISHI TAKAYOSHI

(54) ELECTRONIC TRANSACTION SYSTEM

(57)Abstract:
PURPOSE: To prevent a verifying personnel from running away with an electronic signature of a signer by devising a digital signature in such way that a specific condiction is to be satisfied.
CONSTITUTION: The identification of the concerned personnel is checked twice by executing the confirmation of sender/recipient, addition of certification of contents, provision of pass code and the fact of reply of a terminal equipment as procedures of the transaction. Then the additional verification personnel of a tally impression sending procedure from the verification personnel to a signer receives a massage M from the signer, confirms the content of the message M and approves of the transaction. In this case, the face that a high-order bit string h1 in a compressed ciphered text of the message M is included in the tally impression generated by the verification personnel only is to be confirmed. Thus, the fact is used for a proof if the verification personnel negates the existence of the transaction at the exchange of the electronic signature, does not reply the electronic signature of the verification personnel as a reply and runs away with the electronic signature of the signer.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－254543

⑤1Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和62年(1987)11月6日
H 04 L 9/00		A－7240－5K	
// G 06 F 15/30	330	7208－5B	

審査請求　未請求　発明の数 1　（全10頁）

㊹発明の名称　電子取引方式

㉑特　願　昭61－96705

㉒出　願　昭61(1986)4月28日

特許法第30条第1項適用　昭和60年11月5日　社団法人電子通信学会発行の「昭和60年度電子通信学会情報・システム部門全国大会講演論文集」に掲載

㉒発明者　宝木　和夫　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

㉒発明者　倉敷　信宏　東京都渋谷区道玄坂1丁目16番3号　株式会社日本ビジネスコンサルタント内

㉒発明者　佐々木　良一　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地

㉔代理人　弁理士　小川　勝男　外1名

最終頁に続く

明　細　書

1．発明の名称

電子取引方式

2．特許請求の範囲

1．書類を電気的情報に置き換えて、電子的に所望の取引を行う電子取引方式において、

予め、取引文を非正式に認めたことを示す認証データを作成する第1の認証データ作成方法と、取引文を正式に認めたことを示す認証データを作成する前記第1の認証データ作成方法とは異なる第2の認証データ作成方法を定めておき、第1の取引者（甲とする）と第2の取引者（乙とする）が取引を行う場合に、

甲は、該取引文に対し、第1の認証データ作成方法により、第1の認証データを作成して乙に送信し、乙は、甲より該第1の認証データを受信した後に、該取引文に対し、第2の認証データ作成方法により第2の認証データを作成して甲に送信し、

甲は、乙より該第2の認証データを受信した後に、該取引文に対し、第2の認証データ作成方法により第3の認証データを作成して乙に送信することにより、該取引を成立させることを特徴とする電子取引方式。

2．前記第1の認証データ作成方法は、予め定められた公開鍵暗号方式を用い、取引の状況を示す第1の取引状況データを秘密鍵で暗号化してその暗号文を認証データとする方法であり、前記第2の認証データ作成方法は、予め定められた公開鍵暗号方式を用い、前記第1の取引状況データとは異なる第2の取引状況データを秘密鍵で暗号化してその暗号文を認証データとする方法であることを特徴とする第1項記載の電子取引方式。

3．前記第1の取引状況データは、該取引文を第1の圧縮暗号化方法により圧縮暗号化した第1の圧縮暗号文を含んでおり、かつ、第2の取引状況データは、該取引文を前記第1の圧縮暗号化方法とは異なる第2の圧縮暗号化方法により圧縮暗号化した第2の圧縮暗号文を含んでいる

ことを特徴とする第１項記載の電子取引方式。

３．発明の詳細な説明

〔産業上の利用分野〕

本発明は、書類をコンピュータのメッセージに置き換え、電子的に商取引を行う電子取引方式に関する。

〔従来の技術〕

従来より、契約交渉はサイン，印鑑によりその正当性を認証している。利害関係にあるデータが電子取引のように通信でやりとりされる場合、サイン，印鑑データをそのままディジタル通信に変換して送っても、簡単にコピーされる恐れがあり、認証には使用できない。そこで、通常のサイン，印鑑に相当するディジタル署名が必要になる。ここで、メッセージ認証が署名として有効になるためには、次の３条件を満足しなければならない。

（1）　通信文が第三者によって偽造できない。
（2）　受信者が後で、(a) 受信の事実を否定したり、(b) 受信文を偽造したりできない。
（3）　送信者が後で、(a) 送信の事実を否定したり、(b) 送信文を偽造したりできない。

ディジタル署名を実現する手段として次の方法が提案されている。

（1）　慣用暗号を用いたディジタル署名
（2）　公開鍵暗号を用いたディジタル署名
（3）　ハイブリッド方式によるディジタル署名

次に上記３方法の特徴と問題点を述べる。

（１）慣用暗号を用いたディジタル署名

一般にＤＥＳ方式の暗号を用いたディジタル署名がいろいろ提案されているが、公証機関が必要であったり、送信側と受信側で共通の認証鍵を持つため受信者が署名文を改ざんすることができるという問題がある。このため実用性のある署名方式はまだない。

（２）公開鍵を用いたディジタル署名

ＲＳＡの暗号方式等を用いることにより比較的容易にディジタル署名が実現できる。

第２図に公開鍵暗号によるディジタル署名のフローチャートを示す。

ステップ１０１では、送信者Ａからのメッセージｍを入力する。

ステップ１０２では、メッセージｍを送信者Ａの秘密鍵Ｓ１で復号化した復号文Ｄ（ｍ，Ｓ１）を作成する。

ステップ１０３では、復号文Ｄ（ｍ，Ｓ１）をさらに受信者Ｂの公開鍵Ｒ２で暗号化して、暗号文Ｌ＝Ｅ（Ｄ（ｍ，Ｓ１），Ｒ２）を得て、これを受信者Ｂ宛に送信する。

ステップ１０４では、受信者Ｂ宛の受信データＬを受信者Ｂの秘密鍵Ｒ１で復号化してＤ（ｍ，Ｓ１）を得る。

ステップ１０５では、復号文Ｄ（ｍ，Ｓ１）を送信者Ａの公開鍵Ｓ２で暗号化してもとのメッセージｍを求める。

ステップ１０６では、メッセージｍを受信者Ｂに出力データとして出力する。

このフロー・チャートにおいて、ステップ１０４では、暗号文Ｌは秘密鍵Ｒ１を知らないと解読できない。つまり、Ｒ１を知っているのは受信者Ｂだけである。また、ステップ１０２において、Ｄ（ｍ，Ｓ１）を作れるのは秘密鍵Ｓ１を知っている送信者Ａだけである。したがって、メッセージｍを送信したのは確かにＡであり、メッセージを受け取ったのは確かにＢであるということになる。

さらに、メッセージｍが、通常の文章ではなくランダムなデータであったりした時には、ｍが正当なものかどうか判定しにくい。この対策としてメッセージに送信者の識別名，受信者の識別名，メッセージの通し番号，日付等の付属情報を付けて送信することができる。これにより、署名文をコピーして何度も送るような不正行為を防止することができる。

しかし、ＲＳＡによる方式では、演算が複雑になるため暗号化，復号化に時間がかかり、メッセージが長い場合には問題になる。

（３）ハイブリッド方式によるディジタル署名

この方式は、ＤＥＳの暗号方式の利点とＲＳＡの暗号方式の利点をうまく利用しそれぞれの方式をミックスさせたものである。

通常のメッセージはＤＥＳによる暗号通信で送信し、鍵の配送と認証はＲＳＡの方式を使っている。認証の対象となるメッセージは、先ず、ＤＥＳによるデータ圧縮型暗号化処理を行いハッシュ・トータルを求める。第３図にこの方法を示す。第３図において、次の処理を行う。

ステップ２０１：

入力メッセージＭの先頭からＳ６ビット単位でｎ個に分割し、先頭からＭ１，Ｍ２，…，Ｍｎとする。

$$M = M1, M2, \cdots, Mn$$

ステップ２０２：

Ｍｉ（ｉ＝１，２，…，ｎ）に７ビット単位で１ビットのパリティ・ビットを付加し、それをＫｉ（ｉ＝１，２，…，ｎ）とする。

ステップ２０３：

ｊ＝１，２，…，ｎとして、以下の処理を繰り返す。

・Ｋｊを暗号化鍵として、Ｉ（ｊ－１）を暗号化し、その暗号化結果とＩ（ｊ－１）との排他的論理和をとり、その結果をＩ（ｊ）とする。

$$I(j) \leftarrow I(j-1) \oplus EKj(I(j-1))$$

（但し、Ｉ（０）は、初期値。）

ステップ２０４：

$$H(M) = I(n)$$

最後に得られた暗号ブロック圧縮暗号文Ｈ（Ｍ）に、ＲＳＡ方式によるディジタル署名を行う。

次に第４図により、ハイブリッド方式によるディジタル署名の方法を示す。

送信者３０１は、メッセージ３０２（Ｍ）から前記データ圧縮型暗号処理により短い文字列３０３（圧縮型暗号文＝Ｈ(Ｍ)）を算出し、秘密鍵３０４（ｋ１）を用いて暗号機３０５によりディジタル署名３０６（Ｅ(Ｈ(Ｍ)，ｋ１)）を作成して、受信者３０７へ送信する。受信者３０７がメッセージ３０２と署名３０６が、真性なものであると認めるためには、送信者３０１の公開鍵３０８（ｋ２）を用いて、ディジタル署名３０６を暗号機３０９により復号化して元の文字列３１０（Ｈ(Ｍ′)）を作成するとともに、送信者３０１と同様の方法でメッセージ３０２から文字列３１１（Ｈ(Ｍ″)）を算出する。そうして、この両者をブロック３１２で比較し、結果が一致すれば、送信者３０１が秘密鍵３０４の唯一の所有者であると信じる限りは、メッセージ３０２は真性である。

この方式では、長いメッセージに対するディジタル署名でも、短時間で処理できる。

〔発明が解決しようとする問題点〕

以上述べてきた従来方式は、ディジタル署名の条件である（２）－（ａ）「受信者が後で、受信の事実を否定できない。」を満足していない。つまり、受信者は事後において、そのような受信の事実はないと主張した場合、送信者はそれを否定する証拠を持たない。

本発明の目的は、ディジタル署名におけるこのような従来の欠点を除去したうえで、次の条件を満足する電子取引を実現することにある。

（１）通信文が第３者によって偽造できない。
（２）受信者が後で、(a) 受信の事実を否定したり、(b) 受信文を偽造したりできない。
（３）送信者が後で、(a) 送信の事実を否定したり、(b) 送信文を偽造したりできない。

〔問題点を解決するための手段〕

上記目的を達成するため、本発明では次の手順を該取引において実現する。

１．送受信者の確認
２．内容証明機能の付加

３．秘密鍵の保持と端末応答の事実により、本人であることの二重チェックを行う。

以上１．～３．の詳細については、特願昭６０－１９３７３５号を参照されたい。

４．認証者から署名者への刻印送信手順の追加認証者は、署名者よりメッセージＭを受信し、メッセージＭの内容を確認して、取引に合意する場合、予め定められたデータＩ₀にたいする圧縮暗号文Ｈ（Ｍ）を作成し、さらに、Ｈ（Ｍ）を上位側ビット列ｈ１と下位側ビット列ｈ２に分割（∴Ｈ(Ｍ）＝（ｈ１，ｈ２））して、この上位ビット列ｈ１と時刻データＴを繋げて、刻印認証用データ（Ｔ，ｈ１）を作成する。また、異なるハッシュ関数H_1とH_2に対し、H_1(Ｍ）とH_2(Ｍ）を作成し、ｈ１＝H_1(Ｍ），ｈ２＝H_2(Ｍ）としてもよい。該刻印認証用データを認証者の秘密鍵Ｒ１で復号化し、電子刻印Ｄ（(Ｔ，ｈ１)，Ｒ１）を作成し、これを署名者に該メッセージＭについての取引を行うことへの合意の応答として、署名者へ送信する。署名者は、前記電子刻印Ｄ（(Ｔ，ｈ１)，Ｒ１）を認証者の公開鍵Ｒ２で暗号化して、元の刻印認証用データＥ（Ｄ((Ｔ，ｈ１)，Ｒ１)，Ｒ２）＝（Ｔ，ｈ１）を得る。

〔作用〕

認証者にしか作成できない刻印の中にメッセージＭの圧縮暗号文の上位ビット列ｈ１が含まれている事実を確認することにより、この後の電子捺印の交換時に認証者が、取引の事実を否定し、認証者の電子捺印を応答として返さずに署名者の電子捺印を持ち逃げした場合の証拠とすることができる。

〔実施例〕

第１図は本発明を実施するシステムの一構成例である。

第５図は、第１図の構成において本発明を実施する処理手順を示すフローチャートである。

次に、第４図における各構成要素の動作を第５図のフローチャートに従って述べる。

ステップ５０１：署名者４０１は、メッセージ・ファイル４０２より取引文Ｍを署名者側電子取引装置４０４に入力するとともに、ＩＣカード４０３により自分の秘密鍵Ｓ１と署名者４０１の名前，認証者４２６の名前を入力する。

ステップ５０２：署名者側電子取引装置４０４は、メッセージ用暗号器４０５と記憶装置４０６のメッセージ暗号鍵Ｋを用いて取引文Ｍを暗号化したＥＫ（Ｍ）を作成し、ＥＫ（Ｍ）と署名者４０１の名前，認証者４２６の名前を通信制御装置４１３により認証者側電子取引装置４２３に送信する。

ステップ５０３：署名者側電子取引装置４０４は、圧縮関数器４０７により取引文Ｍを暗号鍵として用い、次のように圧縮暗号文Ｈ（Ｍ）の作成を行う。

（１）Ｈ（Ｍ）は、６４ビットの長さの入力データ（初期値）Ｉ（０）を６４ビットの長さの暗号鍵Ｋ１で圧縮暗号化した６４ビットの長さの出力データである。この暗号方式は、予め定められているとする。また、この暗号方式は、入力データＩ（０）と出力データＨ（Ｍ）があたえられたとき、それらの２つのデータから暗号鍵Ｋ１を求めることは、計算量的に困難なものであるとする。

（２）取引文Ｍを５６ビット長のブロックに区切り、各ブロックをＭ１，Ｍ２，…，Ｍｎとする。最後のブロックＭｎの長さが５６ビットに満たないときは、ビット“０”を残りの箇所に追加して、Ｍｎの長さを５６ビットとする。

（３）前記ブロックに対して、７ビット単位で１ビットのパリティ・ビットを付加し、ブロックの長さを６４ビットに拡張する。拡張された各ブロックをＫ１，Ｋ２，…，Ｋｎとする。

（４）入力データＩ（ｉ－１）を鍵Ｋｉで暗号化したものとＩ（ｉ－１）との排他的論理和をとったものをＩ（ｉ）とする。

$$I(i) = I(i-1) + EK_i(I(i-1))$$

以上の処理をｉ＝１，２，…，ｎについて行う。また、初期値Ｉ（０）は、予め定められた値だと

する。

（５）（４）で最終的に求められた値Ｉ（ｎ）をＨ（Ｍ）とする。また、Ｈ（Ｍ）を上位と下位のデータに分割し、それぞれをｈ１，ｈ２とする。

Ｈ(Ｍ)＝(ｈ１，ｈ２)＝Ｉ(ｎ)

ステップ５０４：認証者側電子取引装置４２３は、メッセージ用暗号器４２２と暗号鍵Ｋを用いて暗号文ＥＫ（Ｍ）を復号化する。

Ｍ＝ＤＫ(ＥＫ(Ｍ))

そして、取引文Ｍを認証者４２６に知らせる。

なお、暗号器を復号器として使うためには、ＲＳＡ方式では鍵を変えればよく、ＤＥＳ方式ではモード指定用スイッチを切り換えればよいので、以下の説明では復号器の場合も単に暗号器と記述する。

ステップ５０５：認証者４２６は、ステップ５０４により復号化された取引文Ｍを見て、取引をしても良いと判断したら、ＩＣカード４２４により自分の秘密鍵Ｒ１を入力する。

ステップ５０６：認証者側電子取引装置４２３は、ステップ５０３と同様の方法により、圧縮関数器４２０を用いて取引文Ｍを圧縮暗号化し、Ｈ（Ｍ）＝（ｈ１，ｈ２）を作成する。また、予め定められた形式に従ったデータを識別記号Ｔとして時刻発生器４１７により作成する。今の場合、識別記号Ｔとして、その時の時刻、例えば、「昭和６０年４月１１日１５時５３分１２秒」を作成する。

ステップ５０７：該識別記号Ｔと分割器４１９により暗号データＨ（Ｍ）から作成した上位データｈ１により、刻印認証用データＷ１を認証データ作成回路４１８を使って作成する。

Ｗ１＝（Ｔ，ｈ１）

ステップ５０８：予め定められた公開鍵暗号方式により、秘密鍵Ｒ１を用いて刻印認証用データＷ１を捺印・刻印用暗号器４１５により復号化し、Ｄ（Ｗ１，Ｒ１）を作成する。そして、Ｄ（Ｗ１，Ｒ１）を署名者側電子取引装置４０４に送信する。

ステップ５０９：署名者側電子取引装置４０４は、記憶装置４０６の認証者公開鍵Ｒ２を用いてＤ（Ｗ１，Ｒ１）を捺印・刻印用暗号装置４１２により暗号化しＷ１′＝Ｅ(Ｄ(Ｗ１，Ｒ１)，Ｒ２)を得る。もし、秘密鍵Ｒ１と公開鍵Ｒ２が正しい暗号鍵と復号鍵の組であるなら、Ｗ１＝Ｗ１′すなわち、Ｔ＝Ｔ′，ｈ１＝ｈ１′が成立することになる。暗号化結果Ｗ１′を比較器４１１によりチェックして、その結果をディスプレイ装置（図示せず）上に表示する。もしも、Ｔ′が予め定められた形式に合致するものであり、ｈ１′が５０３で作成したｈ１と等しいことを示す表示があれば、認証者４２６本人は確かに認証者側電子取引装置４２３にいることを確認する。今の場合、Ｔ′の内容はＴと同じ「昭和６０年４月１１日１５時５３分１２秒」となるので、上記の確認がなされる。

ステップ５１０：署名者４０１は、認証者側電子取引装置４２３に、確かに認証者４２６本人がいて、かつ、認証者４２６は取引文Ｍに対して取引を受け付けても良いと判断したことを知る。そして、自分の電子捺印を作成するため、署名者側電子取引装置４０４のキーボード（図示せず）上に設けた「捺印ＯＫボタン」を押す。

ステップ５１１：署名者側電子取引装置４０４は、認証データ作成回路４０９に５０３で作成した（ｈ１，ｈ２）と５０９で得たＴ′を入力して、捺印認証用データＷ２を作成する。

Ｗ２＝（Ｔ′，ｈ１，ｈ２）

ステップ５１２：予め定められた公開鍵暗号方式により、秘密鍵Ｓ１を用いて刻印認証用データＷ２を捺印・刻印用暗号器４１２により復号化し、Ｄ（Ｗ２，Ｓ１）を作成する。そして、Ｄ（Ｗ２，Ｓ１）を認証者側電子取引装置４２３に送信する。

ステップ５１３：認証者側電子取引装置４２３は、記憶装置４２１の署名者公開鍵Ｓ２でＤ（Ｗ２，Ｓ１）を暗号化したＷ２″を捺印・割印用暗号器４１５により作成する。

$$W2'' = E(D(W2, S1), S2)$$

Ｗ２″＝（Ｔ″，ｈ１″，ｈ２″）としたとき、比較器４１６により、

$$T'' = T, \text{かつ}, (h1'', h2'') = (h1, h2)$$

が成立しているか、確認を行い、その結果を表示して認証者４２６に知らせる。

ステップ５１４：認証者４２６は、ステップ５１３の結果が、「Ｔ″＝Ｔ、かつ（ｈ１″，ｈ２″）＝（ｈ１，ｈ２）が成立」であることを確認したとき、Ｄ（Ｗ２，Ｓ１）は確かに署名者４０１本人が取引文Ｍに基づいて作成したものであると判断し、自分も電子捺印を作成，送信する

成する。

$$W2'' = E(D(W2, R1), R2)$$

Ｗ２″＝（Ｔ″，ｈ１″，ｈ２″）としたとき、比較器４１１を用いて、

$$T'' = T', \text{かつ}, (h1'', h2'') = (h1, h2)$$

が成立していれば、Ｄ（Ｗ２，Ｒ１）は確かに認証者４２６本人が取引文Ｍに基づいて作成したものと判断する。

ステップ５１８：署名者側電子取引装置４０４は、取引文Ｍ，署名者４０１の電子捺印Ｄ（Ｗ２，Ｒ１），認証者４２６の電子捺印Ｄ（Ｗ２，Ｓ１），割印Ｄ（Ｗ２，Ｒ１）をメッセージファイル４０２に記録し、動作を終了する。

ステップ５１９：署名者４０１は、メッセージファイル４０２を保管する。

ステップ５２０：認証者側電子取引装置４２３ことを決定する。そして、認証者側電子取引装置４２３のキーボード（図示せず）上に設けた電子捺印作成・送信用ボタンを押す。

ステップ５１５：認証者側電子取引装置４２３は、５０６で作成した（ｈ１，ｈ２）とＴから、捺印認証用データＷ２を認証データ作成回路４１８により作成する。

$$W2 = (T, h1, h2)$$

ステップ５１６：認証者側電子取引装置４２３は、ＩＣカード４２４による認証者秘密鍵Ｒ１を用いて公開鍵暗号方式により、Ｗ２を復号化したＤ（Ｗ２，Ｒ１）を捺印・割印用暗号器４１５により作成する。そして、Ｄ（Ｗ２，Ｒ１）を署名者側電子取引装置４０４に送信する。

ステップ５１７：署名者側電子取引装置４０４は、記憶装置４０６の認証者公開鍵Ｒ２を用いて、公開鍵暗号方式によりＤ（Ｗ２，Ｒ１）を暗号化したＷ２″を捺印・割印用暗号器４１２により作

は、取引文Ｍ，署名者４０１の電子捺印Ｄ（Ｗ２，Ｓ１），認証者４２６の電子捺印Ｄ（Ｗ２，Ｒ１），割印Ｄ（Ｗ２，Ｒ１）をメッセージファイル４２５に記録後、動作を終了する。

ステップ５２１：認証者４２６は、メッセージファイル４２５を保管する。

実施例の変形例１．

前記実施例のステップ５０１およびステップ５０５において、予め、秘密鍵の一部の情報を磁気カードまたはＩＣカードに記録しておき、秘密鍵の残りの情報を暗証番号の形で当事者が記憶しておき、秘密鍵Ｓ１，Ｒ１を入力する場合には、磁気カードまたはＩＣカードからの情報を読み出しと暗証番号のキー入力により秘密鍵Ｓ１，Ｒ１の入力を実現しても良い。

実施例の変形例２．

前記実施例のステップ５０１，５０５，５１０，５１４のいずれかにおいて、当事者が入力操作を行う前に声紋，指紋等によって本人であることを確認する動作を該当の端末動作に追加しても良い。

〔発明の効果〕

本発明によれば、次の条件を満足する電子取引を仲介機能の介在なしにおこなうことができる。

(1) 第３者は、署名者又は認証者を装って不正に取引をおこなうことはできない。
(2) 認証者は取引文を改ざんできない。
(3) 署名者は、取引成立後、取引文の内容を否定することはできない。

これは、前記（２）で認証者が取引文を改ざんできなかったのと同様の理由による。

(4) 認証者は、署名者の電子捺印を持ち逃げすることはできない。

次の（ａ）により、認証者が署名者の電子捺印を持ち逃げすることはできない。

（ａ）刻印の保持チェック

$$D(W1, R1') = D(W1, R1)$$

となるような、秘密鍵Ｒ１′を作成することが、計算量的に困難なため、該取引文Ｍによる圧縮暗号文の上位側データを含む刻印を作成できるのは、秘密鍵Ｒ１を持つ認証者だけである。

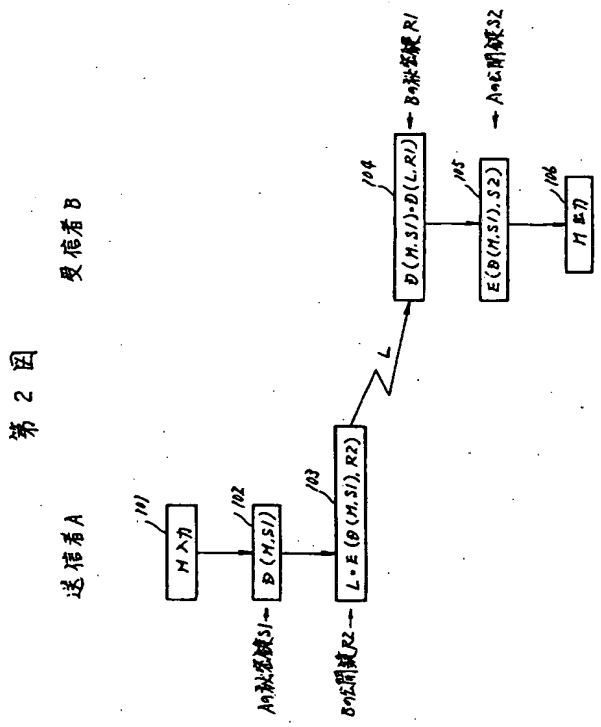
4．図面の簡単な説明

第１図は本発明を実施する一構成例を示す図、第２図は公開鍵暗号方式を用いた従来のディジタル署名方式を示す図、第３図はデータ圧縮型暗号の原理を示す図、第４図はハイブリッド方式によるディジタル署名の方法を示す図、第５図は本発明の処理手順を示すフローチャートであり、本発明を実施する場合における第１図の各構成要素の動作を記述したものである。

署名者と認証者が、取引文Ｍについての電子取引を行っているとき、署名者が、署名者の電子捺印Ｄ（Ｗ２，Ｒ１）を送信した後、認証者が、認証者の電子捺印Ｄ（Ｗ２，Ｒ１）を送信せずに此の取引があったことを否定しようとした場合、署名者は、前記刻印を認証者の公開鍵Ｒ２で復号化して、その内容をチェックすることで、認証者が取引の事実を否定して、署名者の電子捺印を持ち逃げしようとしたことの証拠とすることができる。電子捺印の交換に先立ち、認証者が、署名者に送信した刻印Ｄ（Ｗ１，Ｒ１）の内容には、署名者が送信した取引文Ｍを圧縮暗号化して作成したＨ（Ｍ）＝（ｈ１，ｈ２）の上位側データｈ１がある。

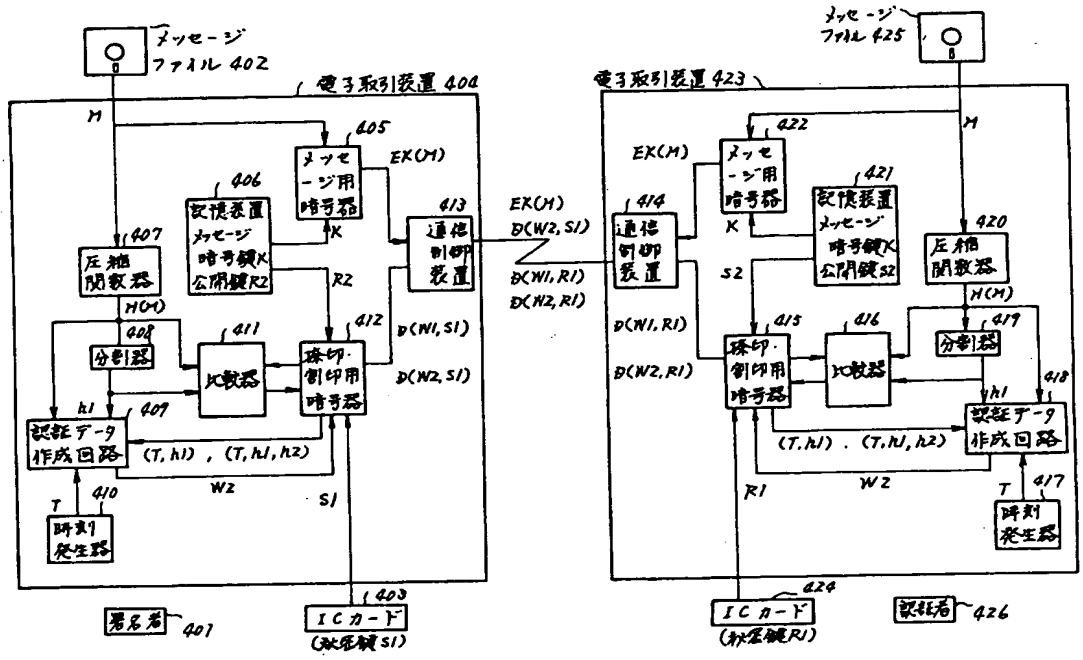
$$W1 = (T, h1)$$

第三者が認証者を装って、不正な取引を行えなかったのと同じ理由により、

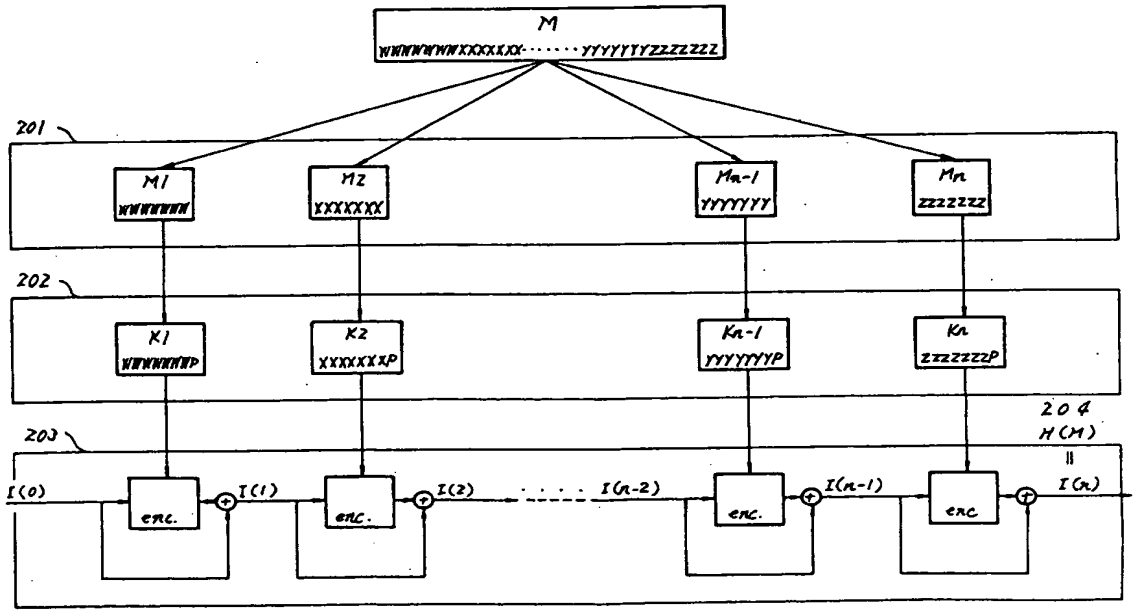


代理人　弁理士　小川勝男

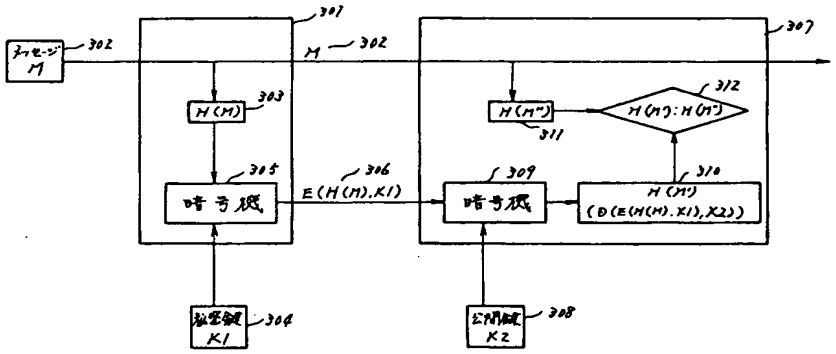
第　1　図


メッセージ
ファイル 402
電子取引装置 404
M
405
メッセージ用暗号器
EK(M)
406
記憶装置
メッセージ暗号鍵K
公開鍵K2
K
K2
413
通信制御装置
EK(M)
D(W2, S1)
D(W1, R1)
D(N2, R1)
407
圧縮関数器
H(M)
408
分割器
411
比較器
412
捺印・創印用暗号器
D(W1, S1)
D(W2, S1)
h1
409
誤証データ作成回路
(T, h1), (T, h1, h2)
W2
S1
T
410
時刻発生器
署名者
401
403
ICカード
(秘密鍵S1)
電子取引装置 423
メッセージファイル 425
422
メッセージ用暗号器
421
記憶装置
メッセージ暗号鍵K
公開鍵S2
420
圧縮関数器
414
通信制御装置
S2
H(M)
D(W1, R1)
D(W2, R1)
415
捺印・創印用暗号器
416
比較器
419
分割器
418
誤証データ作成回路
(T, h1), (T, h1, h2)
R1
W2
T
417
時刻発生器
424
ICカード
(秘密鍵R1)
426

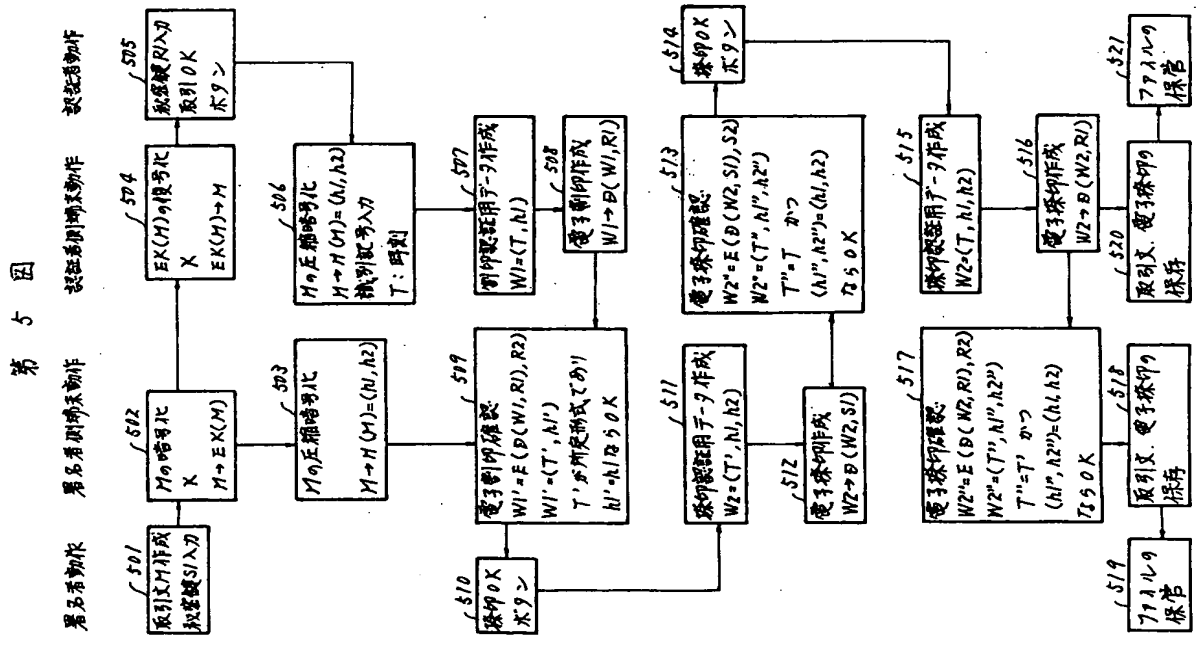
第　3　図


M
WWWWWWWXXXXXXX……YYYYYYYZZZZZZZ
201
M1
M2
Mn-1
Mn
202
K1
K2
Kn-1
Kn
203
204
H(M)
I(0)
I(1)
I(2)
I(n-2)
I(n-1)
I(n)
enc.

第４図


メッセージ M
302
301
M
302
307
H(M)
303
H(M')
311
312
H(M):H(M')
暗号機
305
E(H(M),K1)
306
暗号機
309
H(M')
(D(E(H(M),K1),K2))
310
秘密鍵 K1
304
公開鍵 K2
308

第５図


署名者動作
署名者用端末動作
検証者用端末動作
取引文Mの作成
秘密鍵S1入力
501
Mの暗号化
X
M→EK(M)
502
EK(M)の復号化
X
EK(M)→M
504
秘密鍵R1入力
取引OKボタン
505
Mの圧縮処理
M→H(M)=(h1,h2)
503
Mの圧縮処理
M→H(M)=(h1,h2)
検証用署名入力
T：時刻
506
電子署名作成
W1=(T,h1)
507
電子署名作成
W1→B(W1,R1)
508
電子署名確認
W1'=E(B(W1,R1),R2)
W1'=(T',h1')
T'が所定時刻であり
h1'=h1ならOK
519
電子署名確認
W2'=E(B(W2,S1),S2)
W2''=(T'',h1'',h2'')
T''=T かつ
(h1'',h2'')=(h1,h2)
ならOK
513
電子署名作成
W2=(T',h1,h2)
511
電子署名作成
W2→B(W2,S1)
512
電子署名確認
W2'=E(B(W2,R1),R2)
W2''=(T'',h1'',h2'')
T''=T' かつ
(h1'',h2'')=(h1,h2)
ならOK
517
署名OKボタン
514
署名OKボタン
510
電子署名作成
W2=(T,h1,h2)
515
電子署名作成
W2→B(W2,R1)
516
取引文・電子署名の保存
520
ファイルの保管
521
取引文・電子署名の保存
518
ファイルの保管
519

第１頁の続き

⑫発　明　者　　白　石　　高　義　　川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内